Discrete Mathematics 12 (1975) 211–224.

UNRESTRICTED CODES WITH THE GOLAY PARAMETERS ARE UNIQUE

P. DELSARTE and J.M. GOETHALS
MBLE Research Laboratory, Brussels, Belgium

Received 20 February 1974
Revised 27 August 1974

The paper contains a proof of the uniqueness of both binary and ternary Golay codes, without assumption of linearity. Similar results are obtained about the extended and expurgated Golay codes. The method consists in proving the linearity, which, according to Pless' results, implies the uniqueness.

1. Introduction

Since the discovery by Golay [5] of two remarkable perfect Hamming e-error-correcting codes (for short, e-codes), it has been a challenge for a long time to prove or disprove the existence of other perfect codes. It is only recently that Tietäväinen [12], using some results of van Lint [7], obtained the following very strong result about perfect e-codes of length n over a field alphabet GF(q), for $1 < e < \frac{1}{2}(n-1)$: There are exactly two triples of parameters (e, q, n) for which a perfect code may exist, namely those of the Golay codes (2, 3, 11) and (3, 2, 23), hereafter called the *Golay parameters*.

For $e = \frac{1}{2}(n-1)$, perfect e-codes exist if and only if $q = 2$ and $n \equiv 1 \pmod 2$; such codes simply are formed by any pair of complementary vectors of any odd length over GF(2). On the other hand, perfect 1-codes are known to exist if and only if the length n is of the form $n = (q^r - 1)/(q - 1)$ for some integer $r \geq 2$. Moreover, for each such n, a linear code exists, called the Hamming code [6], which is unique, up to equivalence under monomial transformation of the coordinates. However, there also exist nonlinear perfect 1-codes, as shown by Vasil'ev [13] among others.

So, for $e = \frac{1}{2}(n-1)$ the question of uniqueness is trivial; for $e = 1$ the codes with given (q, n) are in general not unique; and for $1 < e < \frac{1}{2}(n-1)$ we may restrict ourselves to the exceptional sets of Golay parameters, namely

(1.1) $e = 2, \quad q = 3, \quad n = 11$ (the ternary case),

(1.2) $e = 3, \quad q = 2, \quad n = 23$ (the binary case).

Both Golay codes by definition are linear and Pless [9] showed that they are unique as linear codes, in the sense that any linear perfect code with parameters (1.1) or (1.2) is equivalent, under some monomial transformation of its coordinates, to the corresponding Golay code. However, the question remained open whether nonlinear perfect codes with the Golay parameters could exist. This question was partially answered by Snover [10] who showed the uniqueness of the binary Golay code, without assuming linearity.

In this paper, we shall prove the uniqueness of both codes, essentially by showing that they necessarily are linear if they contain the zero vector. The proof is particularly simple in the binary case. In both cases, we use the fact that the distance distribution is uniquely determined from the parameters. Uniqueness of some related codes is also proved in a similar way. In order to make the paper relatively self-contained, we first recall some basic definitions (Section 2), and show how the distance distributions can be uniquely derived (Section 3). The rest of the paper is devoted to the main result, namely a proof of the uniqueness of the ternary and binary Golay codes (Sections 4 and 5, respectively).

2. Definitions and preliminaries

Let $V(n, q)$ denote the vector space of all n-tuples over the Galois field GF(q). We make $V(n, q)$ a normed space by defining the *Hamming weight* w over it:

$$w(x) = |\{i: 1 \leqslant i \leqslant n, x_i \neq 0\}|, \qquad x \in V(n, q).$$

The *Hamming distance* between two vectors x, y then is the weight of their difference: $d(x, y) = w(x - y)$.

A *code* of length n over GF(q) by definition is a nonempty subset of $V(n, q)$, provided with the Hamming metric. Since translation in $V(n, q)$ does not affect the distance relations, we may assume without loss of

generality that the zero vector **0** belongs to the code. For $q = 2$ or 3, we define the following equivalence relation among codes of length n over GF(q), containing **0**: two codes C and D are called *equivalent* whenever there exists a monomial transformation acting on the coordinates, which maps C onto D. (For $q > 3$, this equivalence relation is not appropriate for a discussion of uniqueness: all permutations of nonzero symbols in each coordinate position have to be taken into account.)

A code is said to be *linear* if it is a subspace of $V(n, q)$. Clearly, for $q = 2$ or 3, a code C, with $\mathbf{0} \in C$, cannot be equivalent to a linear code unless it is itself linear.

Let e be an integer, $1 < e < \frac{1}{2}(n - 1)$. Then C is called a *perfect e-code* if the spheres $S_e(\boldsymbol{a})$ of radius e centred at the points $\boldsymbol{a} \in C$, that is,

$$S_e(\boldsymbol{a}) = \{\boldsymbol{x} \in V(n, q): 0 \leqslant d(\boldsymbol{a}, \boldsymbol{x}) \leqslant e\}, \qquad \boldsymbol{a} \in C,$$

form a partition of $V(n, q)$. Equivalently, C is a code of *minimum distance* $\geqslant 2e + 1$ achieving the sphere packing bound

$$(2.1) \qquad |C| \leqslant q^n \Big/ \left(\sum_{i=0}^{e} \binom{n}{i} (q-1)^i \right).$$

As indicated in the introduction, we shall only consider the Golay parameters (1.1) and (1.2), and we shall prove that any perfect code of either type is linear provided it contains the zero vector of $V(n, q)$. Our argument will be based on the following elementary lemma.

Lemma 2.1. *Let C and D be subsets of $V(n, q)$, with $|C| = q^k$ and $|D| \geqslant q^{n-1-k} + 1$ for some integer k. Assume C and D are mutually orthogonal, that is,*

$$\sum_{i=1}^{n} a_i b_i = 0 \quad \text{for all } \boldsymbol{a} \in C, \boldsymbol{b} \in D.$$

Then C is a k-dimensional subspace of $V(n, q)$.

Proof. Let $\bar{C}$ and $\bar{D}$ denote the linear spans of C and D, respectively. Clearly, $\bar{C}$ and $\bar{D}$ themselves are mutually orthogonal. Hence,

$$\dim(\bar{C}) + \dim(\bar{D}) \leqslant n.$$

On the other hand, our assumption on the cardinalities of C and D imply $\dim(\bar{C}) \geqslant k$, $\dim(\bar{D}) \geqslant n - k$. Therefore, the only possibility is $\dim(\bar{C}) = k$

and $\dim(\bar{D}) = n - k$. So we have $C = \bar{C}$, which means that C is a vector space (and D spans the orthogonal complement of C).

The following result can be proved by a similar argument; the details are left to the reader.

Lemma 2.2. *Let C be a self-orthogonal subset of $V(n,q)$, with cardinality $|C| = q^{\lfloor n/2 \rfloor}$. Then C is an $\lfloor \frac{1}{2}n \rfloor$-dimensional subspace of $V(n,q)$.*

We shall also be interested in the so-called *extended perfect codes*, i.e., codes of length $m = n + 1$ and minimum distance $\geqslant 2e + 2$ having the property that the code obtained by puncturing a fixed coordinate becomes a perfect e-code of length n. Such linear codes are known to exist with the parameters (1.1) and (1.2), and their uniqueness has been established, as linear codes, by Pless [9]. Without the assumption of linearity, the uniqueness has been proved only in the binary case, by Snover [10]; the ternary case will be settled in the present paper.

In connection with perfect codes, let us finally mention the "dual" problem of the generalized Hadamard codes (for short, GH codes), introduced by Delsarte [4]. Denoting by s the *number of distances* of a code C, i.e., the number of nonzero values assumed by the Hamming distance between codevectors, we have the following inequality:

$$(2.2) \qquad |C| \leqslant \sum_{i=0}^{s} \binom{n}{i} (q-1)^i.$$

When the bound (2.2) is tight, C is called a *generalized Hadamard code of order s*. It is known that such a linear GH code is nothing but the orthogonal complement of a linear perfect s-code (cf. Delsarte [4]). A general discussion of the admissible parameters of GH codes (linear or not) seems to be more difficult than the corresponding problem for perfect codes. However, for $s = 2$ and 3, the question is settled: there are exactly two sets of parameters for which "nontrivial" GH codes do exist, namely $s = 2$, $q = 3$, $n = 11$ and $s = 3$, $q = 2$, $n = 23$, corresponding of course to (1.1) and (1.2). (Cf. Delsarte [4] for $s = 3$. The case $s = 2$ needs sharper arguments, based on the fact that the distance graph of the code is strongly regular.) In this paper, we shall prove the uniqueness of GH codes of both types, by showing that they must be linear and, therefore, according to Pless' theorems [9], that they are equivalent to the orthogonal complement of the corresponding perfect

Golay code. Let us point out that, in both cases, a linear GH code can be obtained by *expurgating* the associated perfect linear code, or by *shortening* the extended perfect code (cf. Berlekamp [1]).

3. Distance distributions

For each of the three problems mentioned above (perfect codes, extended perfect codes, GH codes), the starting point is the distance distribution which, although it only depends on the parameters, contains interesting "structural" information about the codes. Let us recall the definition. The *distance distribution* of a code C of length n is the $(n+1)$-tuple $\boldsymbol{A} = (A_0, A_1, \ldots, A_n)$, where A_i denotes the average number of codevectors at distance i from a fixed codevector, i.e.,

$$|C|\, A_i = |\{(\boldsymbol{a}, \boldsymbol{b}) \in C^2 : d(\boldsymbol{a}, \boldsymbol{b}) = i\}|.$$

When C is linear, $\boldsymbol{A}$ reduces to the classical *weight distribution*. In fact, the same property holds for any code containing 0 provided it is *distance invariant*, in the sense that the number of codevectors at a given distance from a fixed codevector is independent of this particular vector.

To determine the distance distribution we shall use the *linear programming approach*, restricting our interest to the extended perfect codes. (As for the perfect codes and GH codes, we refer to Delsarte [4].) We shall need the machinery of Krawtchouk polynomials (cf. Szegö [11, p. 35]). For an integer $j = 0, 1, \ldots, n$, we define the *Krawtchouk polynomial of degree j* in the indeterminate z to be

$$P_j(n, z) = \sum_{r=0}^{j} (-1)^r (q-1)^{j-r} \binom{z}{r} \binom{n-z}{j-r}.$$

These form a class of orthogonal polynomials with respect to the weights $w_k(n) = \binom{n}{k}(q-1)^k \; (= P_k(n, 0))$:

$$\sum_{k=0}^{n} w_k(n) P_i(n, k) P_j(n, k) = q^n w_i(n) \delta_{i,j}, \tag{3.1}$$

for all $i, j = 0, 1, \ldots, n$. Another interesting property is the following "symmetry" of the Krawtchouk polynomials:

$$w_k(n) P_i(n, k) = w_i(n) P_k(n, i). \tag{3.2}$$

for $0 \leqslant i, k \leqslant n$. Let k be an integer, $0 \leqslant k \leqslant n$. Then the polynomial

$$L_k(n, z) = P_0(n, z) + P_1(n, z) + \ldots + P_k(n, z) \tag{3.3}$$

is called the *Lloyd polynomial of degree k*. It satisfies $L_k(n, z) = P_k(n-1, z-1)$. (Cf., for instance van Lint [7].)

To a polynomial $F(z)$ with rational coefficients, of degree not exceeding a fixed integer m, we associate its expansion in the basis of Krawtchouk polynomials, that is,

$$F(z) = \sum_{k=0}^{m} \alpha_k P_k(m, z), \tag{3.4}$$

for some well-defined rational numbers α_k. Given an integer δ, with $1 \leqslant \delta \leqslant m$, the polynomial $F(z)$ will be called δ-*positive* whenever it satisfies

$$\alpha_0 > 0, \quad \alpha_1 \geqslant 0, \quad \alpha_2 \geqslant 0, \quad \ldots \quad \alpha_m \geqslant 0,$$

$$F(\delta) \leqslant 0, \quad F(\delta+1) \leqslant 0, \quad \ldots, \quad F(m) \leqslant 0.$$

The main result about the linear programming method is the following theorem, which is valid for an arbitrary q (cf. Delsarte [3]).

Theorem 3.1. *Let C be a q-ary code of length m and minimum distance $\geqslant \delta$. Then, for every δ-positive polynomial $F(z)$,*

$$|C| \leqslant F(0)/\alpha_0 \tag{3.5}$$

holds. Moreover, equality in (3.5) *implies that the distance distribution A of C must satisfy $A_i F(i) = 0$ for all $i \geqslant 1$ and*

$$\alpha_k \left(\sum_{i=0}^{m} A_i P_k(m, i) \right) = 0 \quad \text{for all } k \geqslant 1. \tag{3.6}$$

We shall apply this theorem to codes with even designed distance: $\delta = 2e + 2$. Writing $n = m - 1$, we define the polynomial $F(z)$, from its components α_k in the basis of $P_k(m, z)$, as follows:

$$\alpha_k = (n + 1 - k)(L_e(n, k))^2, \tag{3.7}$$

where L_e denotes the Lloyd polynomial of degree e. Obviously, we have $\alpha_k \geqslant 0$ for $k = 0, 1, \ldots, n+1$, and $\alpha_0 > 0$. Let us determine the values

$F(i)$ at the integral points i between 0 and m. Using the symmetry relations (3.2), we deduce from (3.4),

$$(3.8) \qquad w_i(n+1)F(i) = \sum_{k=0}^{n+1} w_k(n+1)P_i(n+1,k)\alpha_k .$$

Now, by definition (3.7), α_k is a polynomial of degree $2e+1$ in the variable k. Hence, owing to the orthogonality relations (3.1), we deduce that the right member of (3.8) vanishes for all $i \geqslant 2e+2$. This implies that $F(z)$ is δ-positive, for $\delta = 2e+2$.

In order to apply Theorem 3.1, we need $F(0)$. By (3.7) and (3.8), we have

$$F(0) = \sum_{k=0}^{n} (n+1-k)w_k(n+1)(L_e(n,k))^2 .$$

Using the identity $(n+1-k)w_k(n+1) = (n+1)w_k(n)$ and, thereafter, the orthogonality relations, we obtain (see definition (3.3))

$$F(0) = (n+1)\sum_{i,j=0}^{e}\left(\sum_{k=0}^{n} w_k(n)P_i(n,k)P_j(n,k)\right)$$

$$= (n+1)q^n \sum_{i=0}^{e} w_i(n) .$$

On the other hand, (3.7) yields $\alpha_0 = (n+1)(w_0(n)+\ldots+w_e(n))^2$. Hence the linear programming bound (3.5) becomes

$$|C| \leqslant q^n \Big/ \left(\sum_{i=0}^{e} w_i(n)\right) ,$$

i.e., the sphere packing bound (2.1). Accordingly, a code C of length $m = n+1$ and minimum distance $\geqslant 2e+2$ achieves this bound if and only if it is an extended perfect e-code.

Next, we shall make use of the second part of Theorem 3.1 to determine the distance distribution $A = (A_0, A_1, \ldots, A_m)$ of an extended perfect e-code C. Defining

$$(3.9) \qquad B_k = \sum_{i=0}^{m} A_i P_k(m,i) , \qquad 0 \leqslant k \leqslant m\ (=n+1) ,$$

we deduce that B_k vanishes except for $k = 0$, $k = m$ and for the e integers $k = i_1, i_2, \ldots, i_e$ which are the zeros of $L_e(n, z)$; this is an immediate consequence of the definition (3.7), according to the Lloyd theorem on perfect codes (cf., for instance, Delsarte [3,4]).

The values of the nonzero B_k's are calculated as follows. By definition, we have

$$B_0 = |C| = q^n/(w_0(n) + \ldots + w_e(n)) .$$

On the other hand, by similar arguments as in [4, Theorem 6.4], we can express the numbers B_k for $k = i_1, \ldots, i_e$ in terms of the so-called Christoffel numbers associated to the zeros of $L_e(n, z)$. The explicit result, given here without proof, is

$$\frac{(n+1)q^{n-1}}{B_k} = k(n+1-k) \sum_{j=1}^{e} \frac{(L_{j-1}(n, k))^2}{j\, w_j(n)} ,$$

for $k = i_1, i_2, \ldots, i_e$ (= the zeros of $L_e(n, z)$). Then the value of B_{n+1} can be deduced from the above formulas by the identity $\Sigma B_i = q^{n+1}$.

Finally, the distance distribution A is obtained as the solution of the system (3.9), where the B_k's now are well-defined numbers. Using (3.1) and (3.2), we readily calculate

$$(3.10) \qquad q^m A_k = \sum_{i=0}^{m} B_i P_k(m, i) , \qquad 0 \leqslant k \leqslant m\ (=n+1) .$$

(Notice that, for a linear code C, the $(m+1)$-tuple $|C|^{-1} B$ is the weight distribution of the orthogonal complement of C. Then (3.9) and (3.10) are a version of the MacWilliams identities [8].) For the parameters investigated in this paper, namely (1.1) and (1.2), we obtain the following expressions for the *distance enumerators* $A(z) = \Sigma A_i z^i$:

$$(3.11) \qquad A(z) = 1 + 264z^6 + 440z^9 + 24z^{12} \qquad (q = 3),$$

$$(3.12) \qquad A(z) = 1 + 759(z^8 + z^{16}) + 2576z^{12} + z^{24} \qquad (q = 2) ,$$

which are the well-known weight enumerators of the self-orthogonal extended Golay codes.

Let us also write down the distance enumerators of the corresponding perfect codes, for $q = 3$ and $q = 2$, successively:

(3.13) $A(z) = 1 + 132(z^5 + z^6) + 330z^8 + 110z^9 + 24z^{11}$,

(3.14) $A(z) = 1 + z^{23} + 253(z^7 + z^{16}) + 506(z^8 + z^{15}) + 1288(z^{11} + z^{12})$.

As for the corresponding GH codes, the distance enumerators are

(3.15) $A(z) = 1 + 132z^6 + 110z^9$,

(3.16) $A(z) = 1 + 506z^8 + 1288z^{12} + 253z^{16}$.

Let us again emphasize that the distance distribution is constant for all codes in each of the six classes; in other words, it only depends on the parameters.

From the distance distribution A of an arbitrary code C of length m, we define its *dual distance* d' to be the smallest positive integer such that $B_{d'} > 0$, i.e.,

$$\sum_{i=0}^{m} A_i P_{d'}(m, i) > 0.$$

When C is linear, d' is in fact the minimum distance of its orthogonal complement. In general (cf. Delsarte [4]), the integer $t = d' - 1$ is the *maximum strength* of C, i.e., the largest integer having the property that, in each t-subset of coordinate positions, all t-tuples of elements of GF(q) appear a constant number of times (namely, $\lambda = q^{-t}|C|$ times).

In Table 1, the values are given of some important parameters of the codes in which we are interested, like the number of distances s and the maximum strength t. In all cases, we have $t \geqslant s - 1$. This is known to be a sufficient condition for a code to be *distance invariant* (cf. Delsarte [4]). Consequently, for all codes C investigated in the present paper, the weight distribution coincides with the distance distribution, provided we assume $0 \in C$.

Table 1

Parameters of perfect and related codes.

	q	n	$\lvert C\rvert$	s	t
perfect codes	3	11	3^6	5	5
	2	23	2^{12}	7	7
ext. perfect codes	3	12	3^6	3	5
	2	24	2^{12}	4	7
GH codes	3	11	3^5	2	4
	2	23	2^{11}	3	6

4. Uniqueness of the ternary codes

Before examining the ternary "Golay-like" codes, we need some preliminary results. Let $(\boldsymbol{a}, \boldsymbol{b}) = a_1 b_1 + \ldots + a_n b_n$ denote the inner product in $V(n, 3)$. The following useful lemma relates the weights of two ternary vectors, their mutual distance and their inner product.

Lemma 4.1. *For arbitrary vectors* $\boldsymbol{a}, \boldsymbol{b} \in V(n, 3)$,

$$d(\boldsymbol{a}, \boldsymbol{b}) \equiv w(\boldsymbol{a}) + w(\boldsymbol{b}) + (\boldsymbol{a}, \boldsymbol{b}) \pmod 3.$$

Proof. Since the nonzero elements x of GF(3) satisfy $x^2 = 1$, we can write, modulo 3,

$$d(\boldsymbol{a}, \boldsymbol{b}) \equiv \sum_{i=1}^{n} (a_i - b_i)^2 \equiv \sum a_i^2 + \sum b_i^2 - 2\sum a_i b_i$$

$$\equiv w(\boldsymbol{a}) + w(\boldsymbol{b}) + (\boldsymbol{a}, \boldsymbol{b}).$$

Corollary 4.2. *Let* $\boldsymbol{a}$ *and* $\boldsymbol{b}$ *be two vectors in* $V(n, 3)$ *such that the three integers* $\alpha = d(\boldsymbol{a}, \boldsymbol{b})$, $\beta = d(\boldsymbol{a}, -\boldsymbol{b})$ *and* $\gamma = w(\boldsymbol{a}) + w(\boldsymbol{b})$ *are* $\not\equiv 1 \pmod 3$. *Then* $\boldsymbol{a}$ *and* $\boldsymbol{b}$ *are mutually orthogonal, i.e.,* $(\boldsymbol{a}, \boldsymbol{b}) = 0$.

Proof. Writing $\omega = (\boldsymbol{a}, \boldsymbol{b})$, we have, by Lemma 4.1, $\alpha \equiv \gamma + \omega$ and $\beta \equiv \gamma - \omega \pmod 3$. This clearly implies $\alpha + \beta + \gamma \equiv 0 \pmod 3$. According to the hypothesis, the only possibilities are $\alpha \equiv \beta \equiv \gamma \equiv 0$ and $\alpha \equiv \beta \equiv \gamma \equiv -1 \pmod 3$. In both cases, we deduce $\omega \equiv 0 \pmod 3$.

For a given code C we shall denote by C_i the set of codevectors of C having weight i. On the other hand, a code D over GF(3) will be said to be *homogeneous* if $\boldsymbol{a} \in D$ implies $-\boldsymbol{a} \in D$. The following result will be very useful in our proof of the uniqueness of the perfect ternary code.

Lemma 4.3. *Let* C *be any perfect 2-code of length* 11 *over* GF(3), *with* $\boldsymbol{0} \in C$. *Then* C_{11}, C_5 *and* C_6 *are homogeneous.*

Proof. (i) Looking at the distance enumerator (3.13), and remembering that C is distance invariant, we observe that C_{11} contains 24 vectors. On the other hand, C_{11} clearly is a binary code (over $\{1, -1\}$) with minimum distance ≥ 5. Using for instance the linear programming ap-

proach we can determine the distance enumerator of C_{11}:

$$A(z) = 1 + 11(z^5 + z^6) + z^{11}.$$

Since A_{11} is the average number of vectors $-\boldsymbol{a} \in C_{11}$ for $\boldsymbol{a}$ varying through C_{11}, the property $A_{11} = 1$ precisely means that C_{11} is homogeneous. (In fact, C_{11} is the union of a Hadamard code and of its complement; such codes were implicitly investigated by Bose and Shrikhande [2].)

(ii) Let us consider any vectors $\boldsymbol{a} \in C_6$ and $\boldsymbol{b} \in C_{11}$. Since C_{11} is homogeneous, both numbers $d(\boldsymbol{a}, \boldsymbol{b})$ and $d(\boldsymbol{a}, -\boldsymbol{b})$ are distances of C and, therefore (cf. (3.13)), they are $\not\equiv 1 \pmod 3$. Applying Corollary 4.2, we deduce $(\boldsymbol{a}, \boldsymbol{b}) = 0$. Hence C_6 and C_{11} are mutually orthogonal.

(iii) To any given vector $\boldsymbol{a} \in C_5$ we shall now attach a homogeneous set $\{\boldsymbol{b}, -\boldsymbol{b}\}$ of vectors in C_6 which are "disjoint" from $\boldsymbol{a}$, i.e., satisfying $d(\boldsymbol{a}, \boldsymbol{b}) = 11$, as follows: Let L denote the set of coordinate positions i such that $a_i \neq 0$. By definition, $|L| = 5$. Since C forms an orthogonal array of maximum strength $t = 5$ and index $\lambda = 3$ (cf. Table 1), there are exactly 3 vectors $\boldsymbol{x} \in C$ such that $x_i = 0$ for all $i \in L$. One of them being $\boldsymbol{0}$, let $\boldsymbol{b}$ and $\boldsymbol{c}$ denote the other ones. By definition, $d(\boldsymbol{a}, \boldsymbol{b}) = 5 + w(\boldsymbol{b})$. Since $w(\boldsymbol{b})$ must be 5 or 6, and since $d(\boldsymbol{a}, \boldsymbol{b}) = 10$ is excluded, $w(\boldsymbol{b}) = 6$ is the only possibility. Similarly, we have $w(\boldsymbol{c}) = 6$.

Next, we shall prove $d(\boldsymbol{b}, \boldsymbol{c}) = 6$, that is, $\boldsymbol{c} = -\boldsymbol{b}$. Assuming this is false, we would have $d(\boldsymbol{b}, \boldsymbol{c}) = 5$. Then, for a suitable numbering of the coordinates, $\boldsymbol{b}$ and $\boldsymbol{c}$ are as follows:

$$\boldsymbol{b} = (b_1, \ b_2, \ b_3, \ b_4, \ b_5, \ b_6, 0, 0, 0, 0, 0),$$

$$\boldsymbol{c} = (b_1, -b_2, -b_3, -b_4, -b_5, -b_6, 0, 0, 0, 0, 0),$$

where $b_1, \ldots, b_6$ are non-zero. Now, let $\boldsymbol{u}$ be a vector of C_{11}. We have seen in (ii) that $\boldsymbol{u}$ must be orthogonal to $\boldsymbol{b}$ and $\boldsymbol{c}$, whereas our assumption clearly yields $(\boldsymbol{u}, \boldsymbol{b} + \boldsymbol{c}) = -u_1 b_1 \neq 0$. From this contradiction we deduce that the only possibility is $\boldsymbol{c} = -\boldsymbol{b}$.

(iv) Finally, let us show that C_5 and C_6 are homogeneous. We shall use the following equivalence relation (E) on C:

$$\boldsymbol{x} \, E \, \boldsymbol{x}' \quad \text{if and only if } \boldsymbol{x}' = \pm \boldsymbol{x},$$

for $\boldsymbol{x}, \boldsymbol{x}' \in C$. It is obvious that the restriction of E to a given C_i is an equivalence relation on C_i; we define $E(C_i)$ to be any subset of C_i obtained by taking one representative in each class of C_i/E. The above construction (iii) produces as well-defined mapping $\phi : E(C_5) \to C_6/E$

such that

$$\phi(\boldsymbol{a}) = \{\boldsymbol{b}, -\boldsymbol{b}\},$$

with $d(\boldsymbol{a}, \boldsymbol{b}) = d(\boldsymbol{a}, -\boldsymbol{b}) = 11$. It is easily seen that ϕ must be injective. Moreover, since the classes $\phi(\boldsymbol{a})$ contain two elements of C_6, we may write (cf. (3.13))

$$132 = |C_6| \geqslant 2|E(C_5)| \geqslant |C_5| = 132.$$

Hence we deduce $|E(C_5)| = 66$, which means that each class of C_5/E contains two elements, i.e., C_5 is homogeneous. In addition, $|C_6| = 2|E(C_5)|$ clearly implies that ϕ is one-to-one, i.e., C_6 also is homogeneous. This concludes the proof.

We are now able to prove the main result of this paper, namely the uniqueness of the ternary Golay code and some related codes.

Theorem 4.4. *Let C be a code over* GF(3), *containing* **0**, *of the following type, respectively*:

(i) *a* GH *code of order* 2 *and length* 11;
(ii) *an extended perfect* 2*-code of length* 12;
(iii) *a perfect* 2*-code of length* 11.

Then C is equivalent to the following code, respectively:

(i) *the expurgated Golay code*;
(ii) *the extended Golay code*;
(iii) *the perfect Golay code itself.*

Proof. According to Pless' results [9], we only need to show that the codes necessarily are linear.

(i) By (3.15), the distances (and the weights) of C are 6 and 9, so they are $\equiv 0 \pmod 3$. Hence it follows from Lemma 4.1 that C is self-orthogonal: $(\boldsymbol{a}, \boldsymbol{b}) = 0$ for all $\boldsymbol{a}, \boldsymbol{b} \in C$. Then Lemma 2.2 yields the desired result, namely that C is linear.

(ii) By (3.11), the distances of C are 6, 9 and 12. Using the same argument as in (i), we deduce that C is linear.

(iii) First, we observe that C and C_6 are mutually orthogonal. Indeed, by Lemma 4.3, C_6 is homogeneous. Hence (cf. the distance enumerator (3.13)) we may apply Corollary 4.2 to any $\boldsymbol{a} \in C$, $\boldsymbol{b} \in C_6$, thus obtaining $(\boldsymbol{a}, \boldsymbol{b}) = 0$. Next, using Lemma 2.1 with $D = C_6$ (of cardinality 132), we arrive at the conclusion that C is linear.

5. Uniqueness of the binary codes

Not surprisingly, the binary case is simpler than the ternary case. The results we shall now prove were first obtained by Snover [10], who used more sophisticated arguments. Our method is based on Lemmas 2.1, 2.2 and on the following result, the proof of which is by direct verification.

Lemma 5.1. *Let $\boldsymbol{a} \cdot \boldsymbol{b}$ denote the componentwise product of any two vectors $\boldsymbol{a}, \boldsymbol{b} \in V(n, 2)$. Then,*

$$d(\boldsymbol{a}, \boldsymbol{b}) = w(\boldsymbol{a}) + w(\boldsymbol{b}) - 2w(\boldsymbol{a} \cdot \boldsymbol{b}).$$

Theorem 5.2. *Let C be a code over* GF(2), *containing* **0**, *of the following type, respectively:*

(i) *a* GH *code of order* 3 *and length* 23;
(ii) *an extended perfect* 3*-code of length* 24;
(iii) *a perfect* 3*-code of length* 23.

Then C is equivalent to the following code, respectively:

(i) *the expurgated Golay code;*
(ii) *the extended Golay code;*
(iii) *the perfect Golay code itself.*

Proof. Like in the ternary case, we only need to show that the codes are linear (cf. Pless [9]). We shall restrict ourselves to the problem of perfect codes (iii), the other ones being similar (and even simpler). Let D be the subcode of C consisting of all vectors whose weights are $\equiv 0 \pmod 4$. Then, according to (3.14), D contains $1 + 253 + 506 + 1288 = 2^{11}$ vectors.

Given $\boldsymbol{a} \in C$, $\boldsymbol{b} \in D$, we deduce $d(\boldsymbol{a}, \boldsymbol{b}) \equiv w(\boldsymbol{a}) - 2w(\boldsymbol{a} \cdot \boldsymbol{b}) \pmod 4$ from Lemma 5.1, whence

$$\text{either} \quad d(\boldsymbol{a}, \boldsymbol{b}) \equiv w(\boldsymbol{a}) \equiv 0 \pmod 4,$$

$$\text{or} \quad d(\boldsymbol{a}, \boldsymbol{b}) \equiv w(\boldsymbol{a}) \equiv -1 \pmod 4,$$

since, from the distance enumerator, $d(\boldsymbol{a}, \boldsymbol{b})$ and $w(\boldsymbol{a})$ are $\equiv 0$ or $-1 \pmod 4$. Therefore, we have $w(\boldsymbol{a} \cdot \boldsymbol{b}) \equiv 0 \pmod 2$, in both cases. Now this means $\Sigma a_i b_i = 0$ (in GF(2)). Hence the codes C and D are mutually orthogonal, which, by Lemma 2.1, shows that C and D both are linear codes (being the orthogonal complement of each other).

References

[1] E.R. Berlekamp, Algebraic Coding Theory (McGraw-Hill, New York, 1968).
[2] R.C. Bose and S.S. Shrikhande, A note on a result in the theory of code construction, Inf. Control 2 (1959) 183–194.
[3] P. Delsarte, Bounds for unrestricted codes, by linear programming, Philips Res. Rep. 27 (1972) 272–289.
[4] P. Delsarte, Four fundamental parameters of a code and their combinatorial significance, Inf. Control 23 (1973) 407–438.
[5] M.J.E. Golay, Notes on digital coding, Proc. IRE 37 (1949) 657.
[6] R.W. Hamming, Error detecting and error correcting codes, Bell Syst. Tech. J. 29 (1950) 147–160.
[7] J.H. van Lint, Coding Theory, Lecture Notes in Math. (Springer, Berlin, 1971).
[8] F.J. MacWilliams, A theorem on the distribution of weights in a systematic code, Bell Syst. Tech. J. 42 (1963) 79–94.
[9] V. Pless, On the uniqueness of the Golay codes, J. Combin. Theory 5 (1968) 215–228.
[10] S.L. Snover, The uniqueness of the Nordstrom–Robinson and the Golay binary codes, Ph. D. Thesis, Michigan State Univ., East Lansing, Mich. (1973).
[11] G. Szegö, Orthogonal Polynomials, A.M.S. Colloq. Publ. 23 (Am. Math. Soc., Providence, R.I., 1959).
[12] A. Tietäväinen, On the non-existence of perfect codes over finite fields, SIAM J. Appl. Math. 24 (1973) 88–96.
[13] Ju.L. Vasil'ev, On nongroup close-packed codes, Probl. Cybern. 8 (1962) 337–339.